Calendar No. 512

110TH CONGRESS *2d Session* | SENATE | REPORT 110–258

FOREIGN INTELLIGENCE SURVEILLANCE ACT OF 1978 AMENDMENTS ACT OF 2007

JANUARY 22 (legislative day, JANUARY 3), 2008.—Ordered to be printed

Mr. LEAHY, from the Committee on Judiciary, submitted the following

R E P O R T

together with

ADDITIONAL AND MINORITY VIEWS

[To accompany S. 2248]

[Including cost estimate of the Congressional Budget Office]

The Senate Committee on the Judiciary, to which was referred the bill (S. 2248), to modernize and streamline the provisions of the Foreign Intelligence Surveillance Act of 1978 and for other purposes, having considered the same, reports favorably thereon with a substitute amendment, and recommends the bill, as amended, do pass.

CONTENTS

69–010

I. PURPOSE OF THE LEGISLATION

The Foreign Intelligence Surveillance Act of 1978 Amendments Act of 2007, S. 2248, would create additional procedures for targeting communications of persons outside the United States that would significantly enhance the Government's surveillance authority. It moderates the new authorities that Congress granted on a short-term basis in the Protect America Act (PAA), but the bill as reported by the Senate Select Committee on Intelligence would go further than the PAA by providing retroactive immunity for civil lawsuits against electronic communication service providers that were alleged to have cooperated with the Government in surveilling Americans' communications between 2001 and 2007, contrary to law.

The Senate Intelligence Committee reported S. 2248 on October 26, 2007, and the bill was referred sequentially to the Senate Committee on the Judiciary on November 1, 2007, in accordance with section 3(b) of Senate Resolution 400, 94th Congress, as amended by S. Res. 445, 108th Congress, for a period not to exceed 10 days of session.

II. BACKGROUND AND NEED FOR THE LEGISLATION

Congress enacted the Foreign Intelligence Surveillance Act of 1978 as a direct consequence of extensive investigations by Senate Committees into the legality of secret domestic surveillance activities, including Project Minaret, Project Shamrock and the Watergate scandal.[1] These episodes, which involved the United States Government spying on its own citizens, shook the faith of the American people in their Government.

Congress passed FISA to protect the rights of Americans against abusive Government conduct. It mandated that a newly-created independent court must decide whether the Government may conduct electronic surveillance of Americans' communications for foreign intelligence purposes. The FISA court was designed to ensure that a second branch of Government approve or reject the Executive's request to surveil Americans, and the statute erected a legal framework within which the Government, and those private companies the Government relies upon to effectuate electronic surveillance, must operate.

In the years since its passage, FISA has been amended numerous times to accommodate assertions by the Executive that the legislation must keep pace with national security needs as well as technological advancements. For example, in the wake of the 9/11 terrorist attacks, Congress amended FISA to improve communication and coordination between law enforcement and the intelligence community, among other reforms.

In December 2005, the American public learned for the first time that shortly after 9/11 the President had authorized the NSA to conduct secret surveillance activities inside the United States completely outside of FISA, and without congressional consent. Shortly

[1] 1 Project Shamrock was a clandestine Government-run initiative lasting into the 1960s that involved the accumulation by the National Security Agency (NSA) of all telegraphic data entering into or originating from the United States. Project Minaret was a sister program that operated in the 1960s and 1970s that involving the use of "watch lists" to oversee "subversive" domestic activities. Both programs were terminated once congressional investigations exposed their full scope.

after the press exposed the existence of this extra-statutory program, the Administration attempted to justify its operation on the basis of congressional passage of the Authorization for Use of Military Force (AUMF), Pub. L. No. 107–40, section 2(a), 115 Stat. 224 (2001) following the 9/11 attacks. The AUMF, however, made no reference to electronic surveillance, and no legislative history associated with that authorization indicates that it was intended to supersede FISA in any way. Nevertheless, surveillance under this program, commonly referred to as the Terrorist Surveillance Program, or TSP, continued until January 2007, at which time the Attorney General announced that the program would finally be placed under the jurisdiction of the FISA court.

In April 2007, the Director of National Intelligence (DNI), J.M. McConnell, submitted to Congress a proposal to amend FISA in order to make it easier for the Government to target foreign interests overseas. In August 2007, Congress adopted the PAA, which eased restrictions on surveillance of foreigners where one party (or both parties) to the communication are located overseas. Under the PAA, communications that begin or end in a foreign country may be monitored by the Government without FISA court supervision. The PAA was ultimately approved as only a temporary measure with a six-month sunset. Although there was broad support for providing the intelligence community greater flexibility for overseas surveillance, the PAA raised significant concerns because of its lack of any protection for or oversight of communications involving United States persons.

In October 2007, the Senate Intelligence Committee reported a bill, S. 2248, to constitute more permanent legislation supplanting the PAA. The Senate Intelligence bill preserved the general framework of the PAA, but struck or modified some of the PAA's provisions that would have given the Government nearly unfettered authority to collect Americans' communications so long as the Government sought information "concerning" persons outside the United States. The Senate Intelligence bill also included new oversight provisions, but left open several loopholes that could permit the same kinds of extra-statutory surveillance that took place in the years following 9/11. In addition, the Senate Intelligence bill added provisions not formerly included in the PAA that would retroactively immunize those private sector companies that may have cooperated with the Government's surveillance activities conducted outside of FISA in the years following 9/11.[2]

The PAA is set to expire on February 1, 2008. In the Committee's view, as more fully explained below, the Senate Intelligence bill, like the PAA, does not contain adequate protections to guard against the kind of Executive abuse that occurred with the TSP and related programs. Congress is prepared to grant the Administration the authority it needs to surveil targets overseas. But the unilateral decision by the Executive in the years following 9/11 to surveil Americans' communications contrary to FISA illustrates the need for Congress to provide clear statutory protections for surveillance that impacts Americans' privacy rights. Both the Intelligence Committee's bill and the Judiciary Committee's proposed amendments would permit the Government, when targeting overseas, to

[2] For additional information on the specific provisions of S. 2248, see S. Rept. 110–209.

review more Americans' communications with less court supervision than ever before. While the Senate Intelligence bill's provisions governing the Government's ability to conduct electronic surveillance improve upon the PAA, they do not afford adequate protections for the rights of Americans.

Additional protections are of critical importance. The rules governing electronic surveillance affect every American and remain the only buffer between the freedom of Americans to make private communications and the ability of the Government to listen in on those communications. In our "Information Age," FISA provides Americans a fundamental bulwark against Government abuse. In the Committee's view, the improvements contained in the Senate Intelligence bill do not go far enough in ensuring that Americans' privacy rights are safeguarded. Additional protections can be added without interfering with the flexibility the Government needs to conduct overseas surveillance.

III. Scope of Committee Review

The Judiciary Committee has concurrent jurisdiction over the Foreign Intelligence Surveillance Act and all amendments to that Act. The Committee reported S. 2248 favorably, as proposed to be amended by a complete substitute, on November 16, 2007. The complete substitute makes significant improvements to the Senate Intelligence bill by adding several key protections for Americans to title I of the bill that do not compromise the Government's ability to conduct foreign intelligence surveillance. These improvements include: (1) increased oversight by Congress and the FISA court where the Government is conducting warrantless surveillance of targets overseas that will invariably capture Americans' communications; (2) unequivocal new language that FISA is the exclusive means for conducting foreign intelligence wiretaps; (3) improved protections to ensure that Americans who travel overseas do not forfeit their constitutional rights; and (4) appropriate and common sense restrictions against bulk collection and reverse-targeting of Americans' communications to prevent the abuse of the significant new Government powers by this administration or any future administration.

On the key question of immunity, the proposed amendments to the bill preserve prospective immunity for those electronic communications service providers who comply with the law pursuant to title 18, United States Code, section 2511.[3] But the bill as reported does not include the blanket retroactive immunity contained in title II of S. 2248, and legislative termination of litigation efforts by those whose privacy rights may have been violated where private companies, acting together with the Government, arguably ignored the clear statutory guidelines spelled out in FISA and the United States Criminal Code.

Certain of the Committee's proposed changes to S. 2248's title I were initially approved pursuant to a substitute amendment adopt-

[3] Title 18, United States Code, section 2511(2)(a)(ii)(A) and (B) provide, in pertinent part, that providers of wire or electronic communication service are authorized to provide assistance to the Government so long as those providers receive a court order or a certification in writing by the Attorney General or other statutorily designated official stating that no warrant or court order is required by law, that all statutory requirements have been met, and that the specified assistance is required.

ed at the beginning of the November 15th executive session. Other proposed changes to title I were adopted by the Committee as individual amendments later in the session. All Committee changes were approved as part of the complete substitute amendment to S. 2248 that the Committee ultimately adopted on November 16, 2007. For clarity, this report breaks out below each of the individual proposed changes contained in the complete substitute, and describes each individually.

IV. RECOMMENDED CHANGES TO TITLE I OF S. 2248

1. STRENGTHENED ASSERTION THAT THE PRESIDENT MUST COMPLY WITH STATUTES

The Committee proposes an amendment to strengthen the exclusivity language contained in S. 2248 to make absolutely clear that FISA is the sole means by which the Government may intercept Americans' communications for foreign intelligence purposes. The actions and public arguments of the Executive in conducting and later defending the TSP have underscored the importance of inserting an exclusivity provision directly into FISA. The proposed amendment would make clear that the Government cannot claim authority to operate outside of FISA by alluding to legislative measures that were never intended to provide such authority.

The bill as reported by the Senate Intelligence Committee adds a new section to FISA, section 112, which restates the original 1978 language that FISA is the exclusive means by which electronic surveillance will be conducted for foreign intelligence purposes. See FISA Amendments Act of 2007, S. 2248, 110th Cong. (2007) [hereinafter "S. 2248"] § 112. The Committee has revised S. 2248's section 112(a) to address intelligence activities intended to collect the "communications or communications information" of United States persons inside or outside the United States. S. Comm. on the Judiciary, complete substitute to S. 2248 (2007) [hereinafter "Judiciary complete substitute"] § 112(a). This language is not restricted to "electronic surveillance" because that collection is addressed by subsection (b). The term "communications information" in this section is intended to apply to non-content information relevant to a communication that may be acquired through surveillance. The intent of this subsection is to prevent the targeting of the communications of U.S. persons by means other than those defined to be "electronic surveillance" in section 101 of FISA.[4] However, it is not intended to bring into FISA acquisition procedures or techniques that are lawfully used outside of FISA, including those specifically permitted by other statutes.

The Committee's bill also proposes a new subsection (c) to section 112 that makes clear that no future law should be interpreted as having authorized electronic surveillance or overriding FISA unless it does so explicitly. This provision is intended to foreclose any argument, as was made by the Department of Justice in its January 2006 White Paper, that the AUMF constituted a separate authority for surveillance outside of FISA.

[4] The exclusivity language contained S. 2248 has also been modified in subsection (b) of the complete substitute to take into account the striking of the redefinition of "electronic surveillance" in section 701.

In its conforming amendments, the Committee's bill proposes the addition of clarifying language to title 18, United States Code, section 2511, which is the provision allowing the Executive Branch to use a certification to request assistance from electronic communication service providers to conduct surveillance. The current certification language only calls for a declaration that no warrant or order is required, that all statutory requirements have been met, and that the assistance is required. The proposed amendment would mandate that each certification be specific as to why a court order is not required by referencing the applicable statutory provision on which the authority is premised. See Judiciary complete substitute § 102(b). This could include, for example, the provisions in FISA waiving the warrant requirement following a declaration of war.

Ed Black, the President and CEO of the Computer and Communications Industry Association, emphasized the providers' need for clarity in testimony before this Committee. He noted that the providers "must be free to insist on constitutionally solid procedures that are clear and transparent, so that they are not reduced to guesswork about the applicability of immunity under the FISA statute." "Strengthening FISA: Does the Protect America Act Protect Americans' Civil Liberties and Enhance Security?", Hearing before the S. Comm. on the Judiciary, 110th Cong. (2007). If the Government is requesting that an electronic services communications provider assist it in conducting electronic surveillance of Americans, it is entirely reasonable that the Government cite the specific basis for its authority.

Finally, the Committee proposes an amendment that narrows the current language of section 109(a) of FISA, which provides for penalties against anyone who engages in electronic surveillance, or uses or discloses information resulting from electronic surveillance, except as authorized by law. To be consistent with subsection (c), this bill replaces the text "authorized by law" with "authorized by this title or chapter 119, 121, or 206 of title 18, United States Code" in both places that such term appears in section 109(a). Judiciary complete substitute § 102(c).

The Committee believes the involvement of the FISA court is an important protection for U.S. persons' privacy rights, either through the issuance of an order under title I, or through the provisions for the targeting of U.S. persons overseas in section 702. The Committee's intent is to assert the full authorities of Congress under Article I of the Constitution to require that FISA's procedures be followed in all cases where FISA applies.

2. INCREASED OVERSIGHT BY CONGRESS

a. Audit of the President's Warrantless Surveillance Program

The Committee proposes an audit of the TSP and any previous, subsequent or related versions or elements of that program, to be conducted jointly by the Department of Justice Office of Inspector General and the Inspectors General of relevant elements of the intelligence community. Following the completion of the audit, a joint report would then be submitted to the Intelligence and Judiciary Committees in the House and Senate in unclassified form, but with

a classified annex, if necessary. See Judiciary complete substitute § 110.

While certain members of Congress can provide a measure of oversight by familiarizing themselves with classified documents pertaining to the President's warrantless surveillance program, it is important that the relevant Offices of Inspectors General collectively conduct an inquiry to assimilate the key facts and, among other inquiries, to investigate the procedures by which the Department of Justice approved warrantless surveillance of Americans outside of FISA. This is a critical provision for ensuring a full understanding of the actions of the Government in conducting electronic surveillance outside of FISA for several years after 9/11.

The Committee used broad language to describe the scope of the proposed audit for two reasons. First, the Committee was careful not to describe the program beyond what has been discussed publicly to ensure that classified information is not disclosed. Second, the Committee wanted to ensure that the audit covers the full scope of intelligence activities authorized by the President. In a letter to Senator Specter dated July 31, 2007, the DNI acknowledged that the President authorized "various intelligence activities" shortly after 9/11, and that "[a] number of these intelligence activities were authorized in one order." He stated that the "Terrorist Surveillance Program" was "[o]ne particular aspect of these activities, and nothing more. * * *" The letter went on to say that the TSP was "the only aspect of the NSA activities that can be discussed publicly, because it is the only aspect of those various activities whose existence has been officially acknowledged." The broad language used by the Committee seeks to make clear that all of these activities should be included in the audit, and that it not be limited to the "Terrorist Surveillance Program" that the President and others have described previously, and can therefore be discussed.

b. Congressional access to FISA court orders

The bill as reported by the Senate Select Committee on Intelligence, would require that Congress be provided with the orders, decisions and opinions of the FISA court that include significant interpretations of law within 45 days after they are issued. This fills two existing loopholes. First, current law excludes FISA court orders from congressional reporting requirements even though many significant interpretations of law are contained in those orders. Second, semi-annual reporting requirements allow the Government to wait up to a year before informing the Congress about important interpretations of law made by the FISA court. Section 103 requires more timely notification. See S. 2248 §103(c)(1).

The Committee's proposed amendment would also require that Congress be provided the relevant pleadings that may be necessary to understanding the reasoning behind a particular judicial interpretation of the law. See Judiciary complete substitute §103(c)(1). And it would require that significant interpretations of law by the FISA court that were not provided to Congress over the past five years now be provided. See Judiciary complete substitute §103(c)(2). Access to past jurisprudence, as well as current decisions, is critical to Congress's understanding of how FISA is being interpreted and implemented.

3. IMPROVEMENTS TO WARRANT REQUIREMENT FOR AMERICANS OVERSEAS

The Committee proposes certain changes to the provisions contained in S. 2248 relating to Government surveillance of U.S. persons overseas.

The Committee believes that the core features of section 702(c), as passed by the Senate Intelligence Committee, provide important protections for Americans overseas and should be maintained in any final legislation. The Committee's proposed amendment includes further revisions from the language contained in S. 2248 to include an emergency provision that enables the Government to respond to our national security needs immediately, but requires the Government to seek FISA court authorization no later than 72 hours after such surveillance is authorized. See Judiciary complete substitute §702(c)(2)(D). The Committee's proposed amendment also revises the language contained in S. 2248 to provide for a smooth transition from the existing surveillance authorizations conducted under the President's Executive Order 12,333 to the new framework.

Subsection 702(c)(3) requires that the Attorney General submit to the FISA court procedures for determining whether a person outside the United States is in fact a U.S. person. The Court must review these procedures to determine whether they are reasonably designed to determine whether a person outside the United States is a U.S. person.

4. SUNSET

The Committee proposes an amendment to shorten the sunset provision in S. 2248 from six years to four years. In view of the broad new authorities Congress is prepared to approve, four years is a sufficient length of time to revisit whether this increased authority is being exercised appropriately and, conversely, to ensure that the Government has the tools it needs to effectively conduct foreign surveillance. See Judiciary complete substitute §703(c). A four-year sunset will also give the next Administration nearly three years of experience under these new authorities before any reauthorization process.

5. INCREASED OVERSIGHT AND DISCRETION BY THE FISA COURT

The Committee passed three proposed amendments to S. 2248 that would provide for increased judicial oversight over the new authorities contained in S. 2248, and enhance FISA court discretion.[5]

a. Use restrictions

The bill as reported by the Senate Intelligence Committee provides that the FISA court's review of the Government's targeting procedures, minimization procedures, and certifications is not re-

[5] In his minority views, Senator Hatch asserts that the Judiciary complete substitute is "deficient to accomplish the purpose of protecting our nation for a myriad of reasons." But he never explains what those "reasons" are. Instead, he questions only the need for additional oversight by the FISA court, maintaining that there are already sufficient oversight provisions in S. 2248. Senator Hatch writes that the "jurisdiction of the [FISA court] is to grant orders for electronic surveillance," suggesting that he may view the FISA court as nothing more than a rubber-stamp of the Executive will. The Committee does not share this view of the court's role.

quired until after the Government has already implemented those procedures and certifications. See S. 2248 §702(g).

The Committee's proposed amendment states that if the FISA court determines that the Government has been using deficient procedures or certifications to acquire information, its use of the acquired information will be limited in the same way that FISA traditionally limits the use of information acquired under its title I emergency exception if the Government is later turned down for a court order. See Judiciary complete substitute §702(i)(5)(B)(ii)(I). In the Committee's view, there should be at least the potential for consequences if the Executive collects communications using deficient procedures. To prevent the wholesale exclusion of such information in appropriate circumstances, however, the new provision provides increased flexibility by giving the FISA court the authority to allow the continued use of the information under certain circumstances. See Judiciary complete substitute §702(i)(5)(b)(B)(II). In the Committee's view, the FISA court should have the discretion to permit or to exclude the use of communications obtained pursuant to deficient procedures.

b. Continued oversight of Government procedures

Minimization procedures provide a measure of protection for the privacy of U.S. persons. Judicial oversight of how these safeguards are working is a critical element in protecting the privacy of U.S. persons in the area of foreign intelligence surveillance.

The Committee proposes that the FISA court be granted the additional authority to review whether the Government is complying with minimization rules, and be empowered to ask for additional information that is necessary to make its assessment. A new subsection 702(i)(7) would provide the FISA court with explicit authority to review and assess the Government's compliance with the minimization procedures, which are submitted in semiannual reports by the Attorney General and the DNI (and submitted to the FISA court pursuant to section 702(l)(1)). In conducting its review, the court may require the Government to provide additional information regarding the acquisition, retention or dissemination of information concerning U.S. persons during the course of an acquisition.

The Committee also proposes granting the FISA court explicit authority to take remedial action to enforce its orders with regard to minimization compliance and targeting procedures. See Judiciary complete substitute § 702(i)(8). Although the FISA court already has this general enforcement authority, given the court's reduced role in up-front court approval of minimization and targeting procedures, this provision reinforces that enforcement authority with regard to the new procedures in this new title.

c. FISA Court Discretion to Stay Decisions Pending Appeal

The bill as reported by the Senate Intelligence Committee, mandates that if the FISA court finds that the Government has relied on deficient procedures for conducting surveillance under its new authorities, the Government is entitled, in every case, to continue to use those deficient procedures while it is appealing the FISA court's decision to the en banc FISA court and to the FISA court of review. See S. 2248 § 702(i)(6).

In the Committee's view, it is unnecessary and unwise to cabin the FISA court's discretion by imposing a standard mandating that all orders finding Government surveillance procedures to be deficient must be stayed pending en banc and appellate review. The Committee has, therefore, proposed an amendment restoring discretion to the FISA court. Under this provision the Government may move for a stay pending appeal of a FISA court's order to the en banc FISA court or the FISA court of review. See Judiciary complete substitute § 702(i)(6).

6. ELIMINATION OF RE-DEFINITION OF "ELECTRONIC SURVEILLANCE"

The Committee proposes an amendment to eliminate the redefinition of the critical term on which FISA is structured: "electronic surveillance." The PAA and the Senate Intelligence bill both redefine this key term, yet no logical explanation has been offered for why this redefinition is necessary.

This redefinition should be eliminated because it is unnecessary to accomplish the goals of the bill, and it could lead to a variety of unintended consequences. For example, redefining electronic surveillance could potentially nullify FISA's civil and criminal liability provisions for purposes of the new authorities contained in the bill as those provisions are triggered only by unauthorized interception of "electronic surveillance." See 50 U.S.C. §§ 1809, 1810. Suzanne E. Spaulding, a national security expert with 20 years of experience at the CIA and in Congress, echoed this concern in testimony before this Committee when she noted that "[b]y defining out of FISA the acquisition of any communication when it is directed at someone reasonably believed to be outside the United States, you remove any statutory protection that FISA might otherwise provide for Americans whose communications might fall into this category." "Strengthening FISA: Does the Protect America Act Protect Americans' Civil Liberties and Enhance Security?", Hearing before the S. Comm. on the Judiciary, 110th Cong. (2007).

To avoid redefining this key term, the Committee's proposed amendment would affirmatively grant the Government the additional authority it needs to target persons outside the United States in order to acquire foreign intelligence information without an individualized warrant. Judiciary complete substitute § 702(a). This common-sense change explicitly grants the Government the authority it says it needs while avoiding the unintended consequences that may flow from redefining a key term in FISA.

7. PROHIBITION ON BULK COLLECTION

The Director of National Intelligence acknowledged at a Senate Judiciary Committee hearing on September 25, 2007 that the Protect America Act would permit "bulk collection" of all international communications into and out of the United States if the Government had the technological capacity to acquire those communications. See "Does the Protect America Act Protect Americans" Civil Liberties and Enhance Security?", Hearing before the S. Comm. on the Judiciary, 110th Cong., at 82 (2007). Such broad authority goes far beyond what the Government has said it needs and could mean that millions of communications of innocent Americans end up in Government databases.

The Committee proposes that S. 2248 be amended to explicitly forbid bulk collection. Its proposed amendment would require the Government to include in its certification to the FISA court a statement that: "The acquisition is limited to communications to which at least 1 party is a specific individual target who is reasonably believed to be located outside of the United States, and a significant purpose of the acquisition of the communications of any target is to obtain foreign intelligence information." Judiciary complete substitute § 702(g)(2)(vii).

This provision does not require the Government to either identify its individual targets or to explain its interest in the targets to the FISA court. It merely has to make a general certification that there is such an interest and that there are individual targets. In addition, the target need not be named individuals. The target could be, for instance, a phone number, or, if the target is a person, the Government need not know the identity of that person. The Committee also wants to make clear that in an active or projected zone of military combat, the acquisition of communications of any target, known or unknown, would be deemed to have a foreign intelligence purpose by virtue of geographic location if such acquisition is tailored to support such military operations.

The Administration has said that it will use the new authorization granted by FISA for targeted surveillance, not bulk collection. Indeed, warrantless bulk collection of millions of Americans' communications where the Government has no specific interest in the individuals communicating may be unreasonable under the Fourth Amendment. Consistent with the way the Administration has said it plans to use this new authority, this amendment would dispel any concern that this authorization would permit such mass collection and would preserve the Government's ability to target persons overseas.

8. STRENGTHENED PROHIBITION ON REVERSE TARGETING

Reverse-targeting is the prohibited practice of bypassing the FISA court-order requirement by targeting someone overseas in order to mask the Government's actual interest in the U.S. person with whom that foreign target is communicating.

The bill as reported by the Senate Intelligence Committee contains reverse-targeting language requiring a court order when "the purpose" of the surveillance is targeting a person inside the U.S. This language, however, would allow the Government to conduct ongoing, long-term surveillance of an American's communications, without an individualized court order, simply by relying on the fact that the Government is really "targeting" the person overseas with whom the American is communicating.

To ensure that the broad new authorities contained in S. 2248 may not be used to engage in reverse-targeting of Americans, the proposed amendment would require an individualized FISA court order when "a significant purpose of such acquisition is to acquire the communications of a specific person reasonably believed to be located in the United States." Judiciary complete substitute § 702(b)(2) (emphasis added). This prohibition affirms the fundamental and long-standing proposition underpinning title I of FISA that when the Government's interest is in the communications of

a person in the U.S., the Government must conduct this surveillance with a court order based on probable cause.

9. FBI DEPUTY DIRECTOR AS CERTIFYING OFFICIAL

The bill as reported by the Senate Select Committee on Intelligence, would have permitted, without restriction, the Deputy Director of the FBI to be the certifying official on FISA warrants. See S. 2248 §§ 104(1)(D)(ii), 107(a)(1)(E)(ii). The Committee has proposed an amendment that this additional delegated authority be used only when the FBI Director is unavailable. See Judiciary complete substitute §§ 104(1)(D)(ii), 107(a)(1)(E)(ii).

This proposed amendment is not meant to unduly burden the delegation of this function to the Deputy Director of the FBI. It is simply meant to clarify that the certifying official for FISA applications should be, whenever feasible, a politically accountable official who has been appointed by the President and confirmed by the Senate.

V. COMMITTEE ACTION

On November 15, 2007, by vote of 10 ayes and 9 noes, the Committee agreed to adopt a substitute amendment offered by Chairman Leahy and Senators Feinstein, Durbin, Schumer and Whitehouse, which contained several recommended changes to Title I of S. 2248. The votes in person or by proxy were as follows: Chairman Leahy—aye, Senator Kennedy—aye; Senator Biden—aye; Senator Kohl—aye; Senator Feinstein—aye; Senator Schumer—aye; Senator Durbin—aye; Senator Cardin—aye; Senator Whitehouse—aye; Senator Specter—no; Senator Hatch—no; Senator Grassley—no; Senator Kyl—no; Senator Sessions—no; Senator Graham—no; Senator Cornyn—no; Senator Brownback—no; Senator Coburn—no.

Later that morning, by vote of 9 ayes and 10 noes, the Committee rejected an amendment by Senator Specter that would have automatically stayed a FISA judge's order that the Government was using deficient procedures in acquiring communications. The votes in person or by proxy were as follows: Chairman Leahy—no, Senator Kennedy—no; Senator Biden—no; Senator Kohl—no; Senator Feinstein—no; Senator Feingold—no; Senator Schumer—no; Senator Durbin—no; Senator Cardin—no; Senator Whitehouse—no; Senator Specter—aye; Senator Hatch—aye; Senator Grassley—aye; Senator Kyl—aye; Senator Sessions—aye; Senator Graham—aye; Senator Cornyn—aye; Senator Brownback—aye; Senator Coburn—aye.

Later that morning, by vote of 10 ayes and 9 noes, the Committee agreed to an amendment by Senator Cardin that would reduce the sunset for S. 2248 from 6 years to 4 years. The votes in person or by proxy were as follows: Chairman Leahy—aye, Senator Kennedy—aye; Senator Biden—aye; Senator Kohl—aye; Senator Feinstein—aye; Senator Feingold—aye; Senator Schumer—aye; Senator Durbin—aye; Senator Cardin—aye; Senator Whitehouse—aye; Senator Specter—no; Senator Hatch—no; Senator Grassley—no; Senator Kyl—no; Senator Sessions—no; Senator Graham—no; Senator Cornyn—no; Senator Brownback—no; Senator Coburn—no.

Later that morning, by vote of 9 ayes and 10 noes, the Committee rejected an amendment by Senator Specter that would have modified his earlier amendment concerning stays of FISA court orders. The vote in person or by proxy were as follows: Chairman Leahy—no, Senator Kennedy—no; Senator Biden—no; Senator Kohl—no; Senator Feinstein—no; Senator Feingold—no; Senator Schumer—no; Senator Durbin—no; Senator Cardin—no; Senator Whitehouse—no; Senator Specter—aye; Senator Hatch—aye; Senator Grassley—aye; Senator Kyl—aye; Senator Sessions—aye; Senator Graham—aye; Senator Cornyn—aye; Senator Brownback—aye; Senator Coburn—aye.

Later that morning, by vote of 10 ayes and 9 noes, the Committee accepted an amendment by Senator Feingold to clarify that bulk collection of data is not permissible. The votes in person or by proxy were as follows: Chairman Leahy—aye, Senator Kennedy—aye; Senator Biden—aye; Senator Kohl—aye; Senator Feinstein—aye; Senator Feingold—aye; Senator Schumer—aye; Senator Durbin—aye; Senator Cardin—aye; Senator Whitehouse—aye; Senator Specter—no; Senator Hatch—no; Senator Grassley—no; Senator Kyl—no; Senator Sessions—no; Senator Graham—no; Senator Cornyn—no; Senator Brownback—no; Senator Coburn—no.

Later that morning, by vote of 8 ayes and 11 noes, the Committee rejected an amendment by Senator Kyl that would have created a carve-out for overseas warrants where no warrant would have been required in a criminal investigation. The votes in person or by proxy were as follows: Chairman Leahy—no, Senator Kennedy—no; Senator Biden—no; Senator Kohl—no; Senator Feinstein—no; Senator Feingold—no; Senator Schumer—no; Senator Durbin—no; Senator Cardin—no; Senator Whitehouse—no; Senator Specter—no; Senator Hatch—aye; Senator Grassley—aye; Senator Kyl—aye; Senator Sessions—aye; Senator Graham—aye; Senator Cornyn—aye; Senator Brownback—aye; Senator Coburn—aye.

That afternoon, by vote of 10 ayes and 9 noes, the Committee accepted an amendment by Senator Feingold that would require a FISA court order when a significant purpose of targeting someone abroad is to acquire the communications of someone reasonably believed to be in the U.S. The votes in person or by proxy were as follows: Chairman Leahy—aye, Senator Kennedy—aye; Senator Biden—aye; Senator Kohl—aye; Senator Feinstein—aye; Senator Feingold—aye; Senator Schumer—aye; Senator Durbin—aye; Senator Cardin—aye; Senator Whitehouse—aye; Senator Specter—no; Senator Hatch—no; Senator Grassley—no; Senator Kyl—no; Senator Sessions—no; Senator Graham—no; Senator Cornyn—no; Senator Brownback—no; Senator Coburn—no.

That afternoon, by vote of 8 ayes, 10 noes and 1 pass, the Committee rejected an amendment by Senator Kyl that would have created a carve-out for overseas warrants where no warrant would have been required in the U.S. The votes in person or by proxy were as follows: Chairman Leahy—no, Senator Kennedy—no; Senator Biden—no; Senator Kohl—no; Senator Feinstein—no; Senator Feingold—no; Senator Schumer—no; Senator Durbin—no; Senator Cardin—no; Senator Whitehouse—no; Senator Specter—pass; Senator Hatch—aye; Senator Grassley—aye; Senator Kyl—aye; Senator Sessions—aye; Senator Graham—aye; Senator Cornyn—aye; Senator Brownback—aye; Senator Coburn—aye.

That afternoon, by vote of 7 ayes and 12 noes, the Committee rejected an amendment by Senator Feingold that would strike the retroactivity immunity provisions from S. 2248. Chairman Leahy—aye, Senator Kennedy—aye; Senator Biden—aye; Senator Kohl—no; Senator Feinstein—no; Senator Feingold—aye; Senator Schumer—aye; Senator Durbin—aye; Senator Cardin—aye; Senator Whitehouse—no; Senator Specter—no; Senator Hatch—no; Senator Grassley—no; Senator Kyl—no; Senator Sessions—no; Senator Graham—no; Senator Cornyn—no; Senator Brownback—no; Senator Coburn—no.

That afternoon, by vote of 10 ayes and 9 noes, the Committee accepted the substitute amendment to Title I, as amended. The votes in person or by proxy were as follows: Chairman Leahy—aye, Senator Kennedy—aye; Senator Biden—aye; Senator Kohl—aye; Senator Feinstein—aye; Senator Feingold—aye; Senator Schumer—aye; Senator Durbin—aye; Senator Cardin—aye; Senator Whitehouse—aye; Senator Specter—no; Senator Hatch—no; Senator Grassley—no; Senator Kyl—no; Senator Sessions—no; Senator Graham—no; Senator Cornyn—no; Senator Brownback—no; Senator Coburn—no.

That afternoon, by vote of 10 ayes and 9 noes, the Committee accepted a complete substitute amendment to S. 2248, which included Title I and the changes made to that title in Committee, but struck Titles II and III. The votes in person or by proxy were as follows: Chairman Leahy—aye, Senator Kennedy—aye; Senator Biden—aye; Senator Kohl—aye; Senator Feinstein—aye; Senator Feingold—aye; Senator Schumer—aye; Senator Durbin—aye; Senator Cardin—aye; Senator Whitehouse—aye; Senator Specter—no; Senator Hatch—no; Senator Grassley—no; Senator Kyl—no; Senator Sessions—no; Senator Graham—no; Senator Cornyn—no; Senator Brownback—no; Senator Coburn—no.

The next morning, the Committee reconvened and ratified by voice vote its adoption of a complete substitute amendment to S. 2248, and its decision to report the bill, with the proposed amendment, favorably. The Committee proceeded by voice vote to report favorably S. 2248, with the complete substitute as a recommended amendment.

VI. Congressional Budget Office Cost Estimate

DECEMBER 7, 2007.

Hon. PATRICK J. LEAHY,
Chairman, Committee on Judiciary,
U.S. Senate, Washington, DC.

DEAR MR. CHAIRMAN: The Congressional Budget Office has prepared the enclosed cost estimate for S. 2248, the FISA Amendments Act of 2007.

If you wish further details on this estimate, we will be pleased to provide them. The CBO staff contact is Jason Wheelock.

Sincerely,

PETER R. ORSZAG.

Enclosure.

S. 2248—FISA Amendments Act of 2007

Summary: The Foreign Intelligence Surveillance Act Amendments Act of 2007 would make several modifications to the Foreign Intelligence Surveillance Act (FISA) and repeal several sections added to FISA by the Protect America Act of 2007 (Public Law 110–55).

The bill would grant authority to the Attorney General and the Director of National Intelligence (DNI) to authorize surveillance of individuals or groups outside the United States. Such authorizations would permit the incidental acquisition of communications of individuals located within the United States so long as procedures are in place to minimize such acquisitions and to ensure that surveillance is targeted at individuals outside the United States. Under the bill, the Foreign Intelligence Surveillance Court (FISC) would be authorized to review those procedures and to order the government to modify them if the court finds they are inadequate or violate the Constitutional protections against unreasonable search and seizure.

Section 101 of the bill would restrict the ability of the government to target U.S. persons located outside of the United States pursuant to authorizations by the Attorney General and DNI. Under the bill, if the government targets a U.S. person overseas but intends to acquire that individual's communications in the United States, the government must follow the traditional FISA warrant process for electronic surveillance. The bill would require the government to submit an application to the FISC in cases where the government wishes to target a U.S. person overseas intending to acquire that individual's communications outside the United States if that individual had a reasonable expectation of privacy and a warrant would normally be required in the United States. If the government can show that the target is a foreign power or an agent of a foreign power, the bill would authorize the FISC to approve the surveillance.

Since this bill would require the Attorney General and DNI to forward certifications to the FISC regarding the authorization of surveillance of overseas targets and would require the court to review such certifications, the bill would increase discretionary costs associated with such oversight of surveillance programs. However, CBO does not have access to information regarding the amount of surveillance that would be affected by the bill or the current costs incurred by agencies involved with conducting and authorizing such surveillance. Thus, CBO cannot predict how implementing this bill might affect the budget. Any changes in federal spending under the bill would be subject to the appropriation of the necessary amounts. Enacting the bill would not affect direct spending or revenues.

The Unfunded Mandates Reform Act (UMRA) excludes from the application of that act any legislative provisions that are necessary for national security. CBO has determined that the portions of sections 101, 105, and 107 of S. 2248 that would authorize certain electronic surveillance and physical searches without a court order in an emergency situation fall under that exclusion, and CBO has not reviewed those provisions for intergovernmental or private-sector mandates.

Other provisions of the bill contain intergovernmental mandates as defined in UMRA, but CBO estimates that the costs of those mandates to state and local governments would not exceed the annual threshold established in UMRA ($66 million in 2007, adjusted annually for inflation).

S. 2248 also contains a private-sector mandate as defined in UMRA by requiring certain entities to assist the government with electronic surveillance. Because CBO has no information about the prevalence of electronic surveillance and the cost of compliance for entities assisting the government with electronic surveillance, CBO has no basis for estimating the costs of the mandate or whether the costs would exceed the annual threshold established by UMRA for private-sector mandates ($131 million in 2007, adjusted annually for inflation).

Estimated cost to the Federal Government: Since CBO does not have access to information regarding the prevalence of surveillance that would be affected by the bill, or the current costs incurred by agencies involved with conducting and authorizing such surveillance, CBO cannot predict how implementing this bill might affect the budget. Any changes in federal spending under the bill would be subject to the appropriation of necessary amounts. Enacting the bill would not affect direct spending or revenues.

Intergovernmental and private-sector impact: The Unfunded Mandates Reform Act excludes from the application of that act any legislative provisions that are necessary for national security. CBO has determined that the portions of sections 101, 105, and 107 of S. 2248 that would authorize certain electronic surveillance and physical searches without a court order in an emergency situation fall under that exclusion, and CBO has not reviewed those provisions for intergovernmental or private-sector mandates.

Estimated impact on state, local, and tribal governments

Provisions of the bill contain intergovernmental mandates as defined in UMRA, but CBO estimates that the costs of those mandates to state and local governments would not exceed the annual threshold established in UMRA.

If electronic communication service providers comply with certain federal requests for information, the bill would protect them from future liability. Therefore, the bill would preempt some state and local liability laws, and it would eliminate the ability of a public entity to pursue legal action against a service provider. The preemption and the elimination of a legal course of action would be intergovernmental mandates. Information about the nature of existing and potential claims is severely limited, but CBO assumes that few state, local, or tribal governments would act as plaintiffs in such cases. Consequently, we estimate that the costs of the mandates would be small.

The bill also would allow federal law enforcement officers to compel communications service providers, including libraries and other public institutions, to provide information about their customers and users. Based on information from a recent survey of public libraries, CBO estimates that the number of requests and associated costs would likely be small. The bill also would direct the federal government to compensate entities for providing such information.

Estimated impact on the private sector

S. 2248 contains a private-sector mandate as defined in UMRA by authorizing the Director of National Intelligence and the Attorney General to direct certain electronic communication service providers to provide the government with all information, facilities, and assistance necessary to conduct electronic surveillance and to acquire foreign intelligence. Because CBO has no information about how often such entities would be directed to provide assistance or the costs associated with providing assistance, CBO has no basis for estimating the costs of the mandate or whether the costs would exceed the annual threshold established by UMRA for private-sector mandates. The bill also would direct the government to provide compensation, at the prevailing rate, to persons providing information, facilities, or assistance.

Previous CBO estimates: On October 26, 2007, CBO transmitted a cost estimate for the FISA Amendments Act of 2007, as ordered reported by the Senate Select Committee on Intelligence. That version of the bill did not contain the provision found in section 110 of this bill requiring an audit of the "Terrorist Surveillance Program," and authorizing additional personnel for that purpose. To the extent that section 110 would require additional funding for such personnel, the costs associated with implementing this legislation could exceed the costs associated with implementing the version reported by Senate Select Committee on Intelligence. In addition, while both the Intelligence and Judiciary Committees' legislation would protect communication service providers from future liability claims resulting from compliance with federal requests, the earlier version of the bill also included a retroactive liability exemption.

On October 12, 2007, CBO transmitted cost estimates for H.R. 3773, the RESTORE Act of 2007, as ordered reported by the House Permanent Select Committee on Intelligence and the House Committee on the Judiciary on October 10, 2007. Both versions of H.R. 3773 would require the government to apply to the FISC for authorization to conduct surveillance on individuals overseas if such surveillance also would result in the government obtaining the communications of individuals located in the United States. In contrast, S. 2248 would allow the Attorney General and Director of National Intelligence to authorize such surveillance while providing certifications to the FISC that procedures have been put in place to ensure that individuals in the United States are not targeted for surveillance and that the acquisition of communications to or from individuals in the United States is minimized.

Estimate prepared by: Federal Costs: Jason Wheelock; Impact on State, Local, and Tribal Governments: Neil Hood; Impact on the Private Sector: Victoria Liu.

Estimate approved by: Peter H. Fontaine, Assistant Director for Budget Analysis.

VII. Regulatory Impact Evaluation

In accordance with paragraph 11(b)(2) of rule XXVI of the Standing Rules of the Senate, the Committee deems it impractical to evaluate in this report the regulatory impact of provisions of this

bill due to the classified nature of the operations conducted pursuant to this legislation.

VIII. CONCLUSION

The Foreign Intelligence Surveillance Act of 1978 Amendments Act of 2007, S. 2248, as amended by the Judiciary Complete substitute will strike an appropriate balance between Americans' privacy rights and national security prerogatives.

IX. ADDITIONAL AND MINORITY VIEWS

A. ADDITIONAL VIEWS OF SENATOR LEAHY

I write separately to express my view that Congress should not grant retroactive immunity to the electronic communication service providers. I also write to express my support for substituting the United States as the party in interest in the on-going lawsuits against the providers as a possible alternative to retroactive immunity.

I strongly oppose the blanket grant of immunity contained in title II of the Senate Intelligence Committee's bill. By its own acknowledgment, the Administration failed to follow the dictates in FISA by conducting warrantless surveillance of Americans for more than five years. The press uncovered this extra-statutory conduct in late 2005; had it not done so, this unauthorized surveillance may still be going on today. When the public found out that the Government had been spying on the American people outside of FISA for years, the Government and the providers were sued by citizens who believed that their privacy rights were violated. Now, the Administration is attempting to have Congress terminate those lawsuits, perhaps in order to insulate itself from liability. The Senate Intelligence bill would cut off all meaningful accountability by the courts, and would take away the plaintiffs' right to their day in court. We should not allow this to happen.

In running its warrantless surveillance program, the Administration relied on legal opinions prepared in secret and shown only to a tiny group of like-minded officials. Jack Goldsmith, who briefly headed the Justice Department's Office of Legal Counsel, described the program as a "legal mess". This Administration does not want a court to get a chance to look at this "mess," and to determine whether the providers were accomplices to illegal surveillance of their customers. Retroactive immunity would assure that the Administration gets its wish.

Senator Rockefeller and I have fought hard to obtain access to the information that our members need to evaluate whether there is any justification for retroactive immunity. Senator Specter has also worked hard to ensure full disclosure. While these efforts have led to the disclosure of some documents to a limited number of Senators and staffers, it is past time for all other Senators and members of Congress to have access to the entire record in order to make informed judgments about whether to wipe out over 40 ongoing lawsuits.

Senator Rockefeller and I have been cleared to review certain documents about the TSP, but we have drawn very different conclusions about retroactive immunity. I agree with Senator Specter and many others that blanket retroactive immunity, which would

end on-going lawsuits by legislative fiat, undermines accountability and the rule of law.

The arguments in favor of full retroactive immunity do not withstand scrutiny. The Administration and its allies in Congress assert that the providers should be granted immunity based on the common law principle that a private citizen should cooperate when asked to do so by law enforcement. The fundamental flaw in this assertion is that Congress enacted FISA to make clear to the providers what they may and may not do in cooperation with the Government, and Congress already provided for immunity for the providers when they act in accordance with FISA. Given these clear statutory guidelines, the providers cannot now claim a common law defense. That is precisely what the federal district court judge overseeing the consolidated cases against the providers found as a matter of law.

Those arguing for full retroactive immunity point to the possible release of classified information as a reason for short-circuiting the lawsuits. They ignore the fact that federal courts have long had procedures for dealing with classified information in a manner that protects national security. These procedures have been implemented by the federal judge in San Francisco who is handling the bulk of the cases against the providers, and there have been no reported leaks of classified information.

Proponents of full retroactive immunity also argue that if Congress does not terminate the lawsuits against the providers, the providers will not cooperate with legitimate Government surveillance efforts in the future. But this bill would require such cooperation. Moreover, FISA, together with the United States Criminal Code, provide clear guidelines governing when the providers may lawfully cooperate with Government requests for assistance, and there is simply no reason why future providers would ignore these clear statutory guidelines.

If anything, the greater risk is that granting full retroactive immunity will discourage future providers from questioning Government efforts to conduct extra-statutory surveillance because those providers will know that that their lawless conduct can ultimately be nullified by Congress. This would subvert the gatekeeping role that FISA contemplates for the providers. As Jim Dempsey, the Policy Director for the Center for Democracy & Technology, noted at a recent Committee hearing: "[R]etroactive immunity would be inconsistent with the structure and purpose of FISA. FISA was intended to provide clarity to both communications companies and government officials. Retroactive immunity would undermine the role the communications carriers play in effectively checking unlawful surveillance. It would place all carriers in an impossible position during the next crisis. If the government approached them with a request for surveillance that did not meet the statutory requirements, they would be uncertain as to whether they should cooperate in the hope that they would later get immunity. A communications service provider should not have to guess whether cooperation with an apparently illegal request will be excused."

Finally, there is simply no good reason why Congress must act now to deal with the issue of the on-going lawsuits against providers. The claim that these lawsuits will somehow "bankrupt" the

providers is belied by the record demonstrating the financial health of these companies today despite the on-going litigation. Even the most alarmist critics of the lawsuits acknowledge that it will be years, and probably at least two trips to the U.S. Supreme Court, before there are any enforceable final judgments.

While I believe no congressional action is necessary at this time, if there is a clear congressional will to act on this issue in 2008, I would urge members to consider carefully the proposals being developed by Senators Specter and Whitehouse that would substitute the United States for the providers in on-going litigation.

Substitution is a mechanism by which the United States takes the place of private persons or entities in litigation and, in turn, defends the claims against those private parties itself, paying out any resulting monetary damages. Retroactive immunity would effectively quash all on-going cases against the providers. A substitution proposal tailored to these circumstances, however, could allow the plaintiffs to proceed with the essence of their claims against the providers as re-pleaded claims against the United States. While under these unique circumstances plaintiffs may not be able to obtain all of the relief to which they may have been entitled with the providers as party-defendants—such as declaratory or injunctive relief—legal proceedings could move forward against the United States that would entitle the plaintiffs to obtain monetary damages and, importantly, would enable the courts to rule on the legality of the underlying program.

Under classic substitution, the private parties are removed from the litigation entirely. Prior examples of substitution are the National Swine Flu Immunization Program of 1976, Pub. L. No. 94–380, which substituted the Government as defendant in all actions against Swine Flu vaccine manufacturers, and the Atomic Energy Act, Pub. L. No. 101–510, which did the same for claims of injury from exposure to radiation incurred in the course of atomic weapons testing by Government contractors. In these cases, the United States stepped into the shoes of the private parties to defend the tort-based damage claims, and assumed potential liability, because Congress viewed the Government as the true culpable party in litigation.

The United States is immune from civil suit absent an explicit waiver of sovereign immunity. Historically, therefore, Congress has drafted statutes calling for substitution of the U.S. as a party in litigation by waiving sovereign immunity under the framework of the Federal Tort Claims Act (FTCA), 28 U.S.C. §1346(b). The FTCA is a statutory regime that permits civil actions for money damages against the U.S. for injuries caused by the wrongful acts or omissions of a Government employee. The Government sometimes substitutes itself for the defendant and waives sovereign immunity where one of its employees may be liable for tort damages under state law, and the ensuing lawsuits proceed under the FTCA regime. Prior substitution legislation has used this framework because it provides a time-tested means of allowing tort-based private lawsuits to proceed against the Government, and it allows private parties to maintain the exact same claims against the Government that they had maintained against private interests.

The plaintiffs in the lawsuits against the providers have advanced not only state-based tort claims, but also federal statutory claims that are specific to the providers and that may only be brought against private parties. The U.S. cannot, therefore, simply step into the shoes of the providers, as it would do in classic substitution. Rather, given the unique facts here, substitution proposals would have to permit plaintiffs to re-plead their claims so that they may be brought against the Government. The Specter and Whitehouse proposals are drafted to permit such re-pleading.

The Specter and Whitehouse proposals contain an explicit waiver of sovereign immunity, which will allow the lawsuits to proceed against the United States. They also provide for a waiver of the discretionary function exception, which may otherwise exempt the U.S. from civil liability if the conduct of its employees fell within those employees' discretion. And they contain provisions that would make it easier for the plaintiffs to receive discovery from the providers even once those providers are no longer party-defendants.

While I see no need to deal with the issue of lawsuits against the providers in this Congress, I believe that substitution is a fairer means of dealing with these lawsuits than full retroactive immunity, because it would give the plaintiffs their day in court, and it would allow for a measure of accountability for the Administration's actions in the years following 9/11.

PATRICK LEAHY.

B. Additional Views of Senator Feingold

Before leaving town for the August recess this year, Congress passed the Protect America Act (PAA), vastly expanding the government's ability to eavesdrop without a court-approved warrant. That legislation was rushed through without adequate consideration, but it contained a six-month sunset to force Congress to reconsider the approach taken in that bill.

Congress should be taking this opportunity to pass a new bill that allows the government to wiretap suspected terrorists but also protects Americans' basic freedoms. I agree that there is a legislative problem that needs to be addressed. Congress needs to make clear that when foreign terrorists are communicating with each other overseas, the U.S. government does not need a warrant to listen in, even if the collection ends up taking place in this country because of the way modern communications are routed. This purpose can be achieved while protecting the rights and privacy of law-abiding Americans conducting international communications.

S. 2248 as reported by the Senate Select Committee on Intelligence, on which I also serve, falls far short of that goal. In addition, it provides sweeping, unjustified retroactive immunity to those alleged to have cooperated with the President's warrantless wiretapping program. Fortunately, the Senate Judiciary Committee has considered S. 2248 on sequential referral and made significant improvements. While I still have concerns about the bill, I strongly support the changes made in the Judiciary Committee.

The Judiciary Committee version of S. 2248 addresses a number of deficiencies in the Intelligence Committee product. First, I was pleased that the Judiciary Committee adopted an amendment that I offered to rectify a significant problem with the Intelligence Committee bill: it does not clearly prohibit the government from using this new authority to engage in the "bulk collection" of international communications. Bulk collection is the acquisition of large quantities of communications beyond those of individual targets, and could involve the acquisition of all international communications between the U.S. and overseas. The Director of National Intelligence confirmed during the September 25, 2007, hearing of this Committee that the PAA, and presumably the Intelligence Committee bill as well, authorizes bulk collection.

Americans understand that if they talk to a criminal suspect or a terrorist overseas, their conversations might be overheard by the government. What Americans do not expect is that all their international conversations could be wiretapped. Bulk collection goes far beyond the "surgical" approach the Administration has publicly stated that it takes with respect to foreign targeting. According to the Director of National Intelligence (DNI) in an interview with the El Paso Times this summer, "Now there's a sense that we're doing massive data mining. In fact, what we're doing is surgical. A tele-

phone number is surgical. So, if you know that number, you can select it out."

My amendment simply clarifies that the government must have specific targets when it conducts surveillance using these authorities. It need not specify those targets to the FISA Court, nor do the targets have to be known or named individuals. They can, for instance, be telephone numbers, as described by the DNI. Finally, the amendment does not limit collection in support of military operations. As the Committee Report states, "in an active or projected zone of military combat the acquisition of communications of any target, known or unknown, would be deemed to have a foreign intelligence purpose by virtue of geographic location if such acquisition is tailored to support such military operations."

Second, the Judiciary Committee bill contains an additional protection for Americans included in an amendment that I offered. It ensures that the government cannot engage in "reverse targeting"—avoiding FISA's court order requirement by targeting an individual overseas in order to acquire the communications of a person in the U.S. with whom the foreign target is communicating. It requires that a FISA court order be obtained if "a significant purpose" of wiretapping an individual abroad is to acquire the communications of a person reasonably believed to be in the United States. The DNI has stated that reverse targeting, which he defined as wiretapping an individual overseas when the government really wants to listen to an American with whom the target is communicating, violates the Fourth Amendment. This amendment merely codifies this fundamental constitutional principle.

The Judiciary Committee bill also provides a greater oversight role for the FISA Court in a number of respects. It allows the FISA Court to impose restrictions on the use and dissemination of information about Americans that was acquired through procedures the FISA Court later determines to be unlawful. It allows the FISA Court to assess on an ongoing basis the government's compliance with minimization procedures and to ask for additional information to make that assessment. And it makes explicit the FISA Court's authority to take remedial action to enforce its orders and to enforce compliance with those orders.

These changes and others help put the bill on stronger constitutional footing. But troubling aspects of the Intelligence Committee bill remain. Most importantly, the bill does not adequately protect Americans whose communications are intercepted through the use of these new authorities against foreign targets. The scope of the new warrantless collection authorities provided by the Intelligence Committee bill goes far beyond what is commonly understood. The bill would allow the government to listen to communications between Americans in the United States and their friends and colleagues abroad without judicial oversight, even if no party to the communication has any connection to terrorism or any other criminal activity.

While the government must be "targeting" an individual overseas to invoke these authorities, the overseas target need not be a terrorism suspect or be under any suspicion of wrongdoing. The only requirement is that the purpose of the acquisition be to gather "foreign intelligence information," a term with an extremely broad defi-

nition that includes anything relating to foreign affairs. And this broad surveillance is permitted regardless of whether the target is speaking to individuals overseas or individuals in the United States. That means that the government could secretly monitor the communications of an American reporter talking to sources overseas, or an American e-mailing relatives or friends abroad, without a court order or any other any meaningful protections for those Americans. This is perhaps the most serious problem with the Intelligence Committee bill.

It is also a very substantial problem. International communications are now an everyday experience for many Americans. Thirty years ago, when Congress was first considering FISA, it was very expensive, and not very common, for most Americans to make an overseas call. Now, particularly with email, such communications are commonplace. Millions of ordinary Americans communicate with people overseas for legitimate personal and business reasons. Students email friends they have met while studying abroad. Business people communicate with colleagues or clients overseas. Reporters have sources all over the world. Technological advancements combined with the ever more interconnected world economy have led to an explosion of international contacts.

Those who want to give the government new powers often argue that FISA needs to be brought up to date with new technology. But changes in technology should also cause Congress to take a close look at the need for greater protections of the privacy of our citizens. If we are going to give the government broad new powers that may very well lead to the collection of vast quantities of information on innocent Americans, we have a duty to protect their privacy as much as we possibly can. And I believe we can do that without sacrificing any of the efficacy of these new powers for collecting information that will help protect our national security. Unfortunately, neither the Intelligence Committee bill nor the Judiciary Committee bill adequately do so.

In addition, in one very significant respect, the Intelligence Committee bill is far worse than the PAA. It provides retroactive immunity to companies that allegedly cooperated with the illegal warrantless wiretapping program set up secretly after 9/11—an illegal program that continued for more than five years.

I am strongly opposed to this unjustified grant of immunity, which is why I offered an amendment in the Judiciary Committee to strike the retroactive immunity provisions of the bill. Granting retroactive immunity is unnecessary. Current law already provides immunity from lawsuits for companies that cooperate with the government's request for assistance, as long as they receive either a court order or a certification from the Attorney General that no court order is needed and the request meets all statutory requirements. This limited immunity already protects companies that act in good faith while also protecting the privacy of Americans' communications. There is no reason to grant companies that allegedly cooperated with the program a new form of retroactive immunity that undermines the law that applied during the course of this illegal program. It sends a message that Congress does not intend its laws to be followed. And it might very well prevent the courts from ruling on the warrantless wiretapping program. I was disappointed

that my amendment to strip this provision failed, but heartened that six of my colleagues joined me in supporting it.

Finally, I want to express my support for the open process that the Judiciary Committee used to consider this legislation, including an open markup and open hearings. There is no question that some of the Intelligence Committee's work must be conducted behind closed doors due to the sensitive nature of the information it handles on a regular basis. But there should be broader participation in the process of considering changes to this critically important law that has such serious implications for Americans' constitutional rights.

In conclusion, I am pleased with the progress made in the Judiciary Committee. I voted to report the bill because of the improvements it made to the Intelligence Committee bill and because, in the end, the Committee elected not to address Title II of the Intelligence Committee bill, which included the immunity provision. However, I continue to believe that additional improvements are necessary.

RUSSELL D. FEINGOLD.

C. Minority Views of Senator Specter

I agree strongly with the view that Congress must update the Foreign Intelligence Surveillance Act ("FISA") to provide the Intelligence Community with the tools necessary to track foreign terrorists. We must craft a legal framework that provides the Government with the flexibility to respond quickly to emerging threats, while protecting the civil liberties of Americans at home and abroad.

I write separately to express my hope that certain provisions of the Judiciary Committee substitute amendment will be improved and considered individually when the full Senate debates this legislation. I also write to underscore my support for a provision that would substitute the United States Government as the party defendant in place of the communications companies that have been sued for their alleged assistance with the Terrorist Surveillance Program, as an alternative to either retroactive immunity or congressional inaction.

The Judiciary Committee substitute amendment

The Judiciary Committee substitute amendment was adopted on a party-line vote of 10 to 9. Nevertheless, I believe several individual provisions of the substitute amendment, especially if modified to address specific concerns articulated by the Administration and Members of the Minority, could attract bipartisan support in the full Senate. For example, the Committee substitute makes several changes to the so-called Wyden amendment, which requires a court order upon a showing of probable cause for electronic surveillance of United States persons overseas. These changes, including the addition of an emergency exception modeled on existing FISA procedures, should be a welcome improvement to the bill passed by the Select Committee on Intelligence. Likewise, although the substitute's current provision on the exclusivity of FISA may be overbroad, it includes a new subsection intended to clarify that future congressional enactments should not be interpreted as authorizing electronic surveillance or amending FISA unless they do so explicitly. This subsection is similar to language in a bipartisan bill I introduced with Senator Feinstein earlier this year, S. 1114, and should be embraced by those who do not believe the September 2001 Authorization for Use of Military Force (Pub. L. 107–40) constituted a separate authority for surveillance outside of FISA.

It is my view that these and other provisions of the Judiciary Committee substitute, particularly those concerning enhanced congressional oversight and the ability of the Government to continue surveillance after an adverse ruling by a single FISA Court judge, could and should be modified so as to win broader support. I intend to work with Chairman Leahy before final passage of the FISA leg-

islation to achieve this goal, because I believe that Congress must act in a bipartisan way on matters of national security.

Substitution of the Government for communications carriers in pending litigation

I regret that the Judiciary Committee substitute did not deal directly with the question of whether communications carriers alleged to have assisted the Government with the Terrorist Surveillance Program ought to receive some relief from liability. I circulated an amendment on this topic, but it was not considered during the Committee's consideration of FISA reform. Therefore, I subsequently modified and introduced the measure as a stand alone bill, S. 2402. With the agreement of Chairman Leahy, my bill was considered by the Judiciary Committee at the December 13, 2007 executive business meeting. The bill was not approved by the Committee. Nevertheless, I believe that, as my colleagues become more familiar with its provisions, it will gain wider acceptance by the Senate.

The bill, S. 2402, proposes a responsible alternative to the retroactive immunity proposed in S. 2248. It would simultaneously protect the telecommunications providers who assisted the government, while not depriving litigants of their day in court.

The bill substitutes the United States in place of any electronic communication service provider who provided assistance in connection with an intelligence activity that was (1) authorized by the President between September 11, 2001 and January 17, 2007, and (2) designed to detect or prevent a terrorist attack against the United States. For substitution to apply, the electronic communications service provider must have received a written request from the Attorney General or the head of an element of the intelligence community indicating that the activity was authorized by the President and determined to be lawful. The Government will also be substituted if the Attorney General certifies that the electronic communications service provider did not provide the alleged assistance. If, however, the provider assisted the Government beyond what was requested in writing, the bill would provide no relief for such assistance.

At the constructive urging of Senator Whitehouse, the bill also requires, as a precondition for substitution, a determination by the FISA Court that the written request received by the carrier met the statutory standard in title 18, United States Code, section 2511, for surveillance without a court order or that the carrier's assistance was undertaken with a reasonable belief that it was lawful. Once substitution occurs, Federal and state courts are directed to dismiss the providers from the action.

The bill protects the carriers against liability without damaging the litigation interests of legitimate plaintiffs. Specifically, S. 2402 provides that plaintiffs in these cases may continue to send third-party discovery requests to the communications providers after the providers have been dismissed. Moreover, the bill states that plaintiffs may deem provider admissions as Government admissions in their cases against the Government. This bill also establishes a limited waiver of sovereign immunity intended to ensure that the Government can only assert those defenses the communications

companies may assert under current law. On the other hand, nothing in the bill is designed to increase or diminish the ability of the Government to assert the State Secrets privilege, which has already been asserted in the pending litigation. Again, it is my hope that my colleagues will familiarize themselves with this alternative to retroactive immunity before the full Senate considers FISA reform legislation.

ARLEN SPECTER.

D. MINORITY VIEWS OF SENATORS KYL, HATCH, GRASSLEY, SESSIONS, GRAHAM, CORNYN, COBURN, AND BROWNBACK

> The [Fourth Circuit in the *Truong* case], as did all the other courts to have decided the issue, held that the President did have inherent authority to conduct warrantless searches to obtain foreign intelligence information. * * * We take for granted that the President does have that authority and, assuming that is so, FISA could not encroach on the President's constitutional power.

—*In re Sealed Cases,* 310 F.3d 717, 742 (FISA Ct. of Review 2002).

> [The rule that private citizens acting in good faith to assist law enforcement are immune from suit ensures that] the citizenry may be called upon to enforce the justice of the State, not faintly and with lagging steps, but honestly and bravely and with whatever implements and facilities are convenient and at hand.

—*Babbington* v. *Yellow Taxi Corp.,* 250 N.Y. 14, 17 (1928) (Cardozo, J.).

> Whatever has happened to this, someday someone will die and, wall or not, the public will not understand why we were not more effective in throwing every resource we had at certain problems.

—Email from FBI Agent in New York Field Office to FBI Headquarters, August 2001, responding to Headquarters' refusal to allow criminal investigators to search for Khalid al-Mihdhar, Nawaf al-Hazmi, and two other "Bin Laden-related individuals" known to be in the United States prior to the September 11 attacks, because of concerns about violating legal rules segregating intelligence and criminal investigations.

The reason why Congress needs to enact a FISA bill is simple and straightforward: technology has outpaced the law. We are now able to collect intelligence in ways that were never understood or contemplated nearly 30 years ago when the FISA law was drafted. As a result, we need to change the law to accommodate that intelligence collection. Before we changed the law last year, U.S. intelligence agencies had lost about two-thirds of their ability to collect communications intelligence against al-Qaida. Obviously, in this war, we cannot cede two-thirds of the battlefield to the terrorists.

When we enacted the Protect America Act last summer, we regained the capability to collect communications intelligence about al-Qaida by conforming the legal procedures to the technology that enables us to collect this material. Let there be no doubt that the collection of this information as a result of the PAA is critical to our nation's security. In a *New York Times* op-ed on December 10, Michael McConnell, the Director of National Intelligence, noted

that "[i]nformation obtained under this law has helped us develop a greater understanding of international Qaeda networks, and the law has allowed us to obtain significant insight into terrorist planning." Similarly, on October 31 of this year, Kenneth Wainstein, the Assistant Attorney General in charge of the Justice Department's National Security Division, testified before the Judiciary Committee that "since the passage of the [Protect America] Act, the Intelligence Community has collected critical intelligence important to preventing terrorist actions and enhancing our national security."

Al-Qaida has not ceased to exist in years since the September 11 attacks and the fall of the Taliban. Al-Qaida still exists and still desires to carry out the same kinds of attacks against the United States and other countries that it executed on September 11, 2001. We know the incredible amount of damage that can be inflicted if we do not monitor and respond to this threat. We also know that the best way to deal with al-Qaida and the like is to collect intelligence so that we can prevent attacks from occurring in the first place, rather than trying to respond to them after they have occurred. That is why it is so important for Congress to ensure that under the law, the United States can engage in the kind of intelligence collection against al-Qaida that technology today allows.

Many members of the Senate Majority insist that there be stringent congressional oversight of these intelligence-collection programs. No one disputes that point. All agree that we need oversight over the intelligence agencies. That is why this Congress and previous Congresses have agreed on a bipartisan basis to create robust oversight of U.S. intelligence gathering, even when such intelligence gathering is directed at foreign targets. The agencies executing wiretaps and conducting other surveillance must report their activities to Congress and to others, so that opportunities for domestic political abuse of these authorities are eliminated.

The Intelligence Committee bill

The Intelligence Committee worked hard to address the problems posed by changes in communications technology and, after numerous hearings and countless hours of internal deliberations, produced a serious effort to solve these problems. The strength of that committee's effort to work together to improve FISA is apparent in the 13–2 vote by which the committee was able to report a bill. That committee deserves to be commended for its efforts.

Nevertheless, the Intelligence Committee bill is not perfect. To cite one example, the bill includes a provision, adopted via an amendment over the objection of both the Chairman and the Ranking Member, this has come to be called the Wyden amendment. This provision, as written, would require a warrant for any overseas surveillance that is conducted for foreign intelligence purposes and that targets a U.S. citizen or a foreign national who holds a U.S. green card.

The Wyden amendment is unnecessary, it is overly broad, and it threatens to undermine overseas intelligence gathering. First, it is important to emphasize that we already have protocols in place to limit overseas surveillance that is targeted at U.S. persons and to minimize any potential abuses that might result from such surveil-

lance. Section 2.5 of Executive Order 12333 permits surveillance targeting of a U.S. person overseas only if the U.S. Attorney General makes a finding that there is probable cause to believe that the person is an agent of a foreign terrorist organization or other foreign power. The advocates of the Wyden amendment have cited no evidence that this authority has ever been abused by the Intelligence Community.

The Wyden amendment is also overly broad. Under current law, a warrant generally would not be required for overseas surveillance targeted at a U.S. person if the surveillance is conducted for purposes of a criminal investigation.[6] The Wyden amendment thus creates the anomalous situation in which a warrant would be required in order to monitor an overseas terrorist group that includes some U.S. citizens or green-card holders, but no warrant would be required to monitor the very same people—or even a group composed exclusively of U.S. citizens—if that group were suspected of drug trafficking or money laundering. It should not be more burdensome to monitor al-Qaida than it is to monitor a drug cartel. Yet the Wyden provision literally would create a situation in which if an overseas group that includes U.S. persons is suspected of smuggling hashish, no warrant is required, but if the same overseas group is suspected of plotting to blow up New York City, then a warrant would be required. This is absurd.

The Wyden amendment is also likely to undermine overseas counterterrorism investigations by hindering cooperation with foreign intelligence services. In many cases, the best intelligence that the United States obtains about al-Qaida comes from foreign governments' intelligence agencies. Particularly in the Middle East, these governments frequently are afraid of al-Qaida or of radicalized elements of their own populations, and they are quite anxious to ensure that it not be made known that they are cooperating with the United States in the war with al-Qaida. Thus when these foreign governments share intelligence with the United States, they often demand strict assurances that the information will not be disseminated outside of the U.S. Intelligence Community.

If U.S. agents conducting an overseas search in cooperation with a foreign intelligence service will now, as a result of the Wyden amendment, be required to disclose and justify the search to the FISA court, those agents will also need to inform their foreign counterparts that cooperation with the United States will be disclosed to a court. It is already anticipated that these foreign intelligence agencies will be unenthusiastic about working with the United States if the fact of such cooperation will be disclosed in judicial proceedings. It is inevitable that the Wyden requirement will cost the United States information and cooperation from foreign intelligence services—possibly including valuable information that is not available from any other source.

Finally, the Wyden amendment raises the specter that U.S. agents will be required to prove to a U.S. court that overseas intel-

[6] As Kenneth Wainstein noted in his October 31, 2007 testimony before this committee, "[t]he Government is not required to obtain a warrant to collect evidence outside the United States when its purpose is to build a criminal case—where the expected end of the investigative process is often the criminal prosecution of that United States person."

ligence activities comply with foreign law. As Ken Wainstein noted in his October 31, 2007 Judiciary Committee testimony, by "extending this new role to the FISA Court and requiring the court to approve acquisitions abroad [, the Wyden amendment] could cause that court to feel compelled to analyze questions of foreign law as they relate to [such overseas intelligence gathering]."

The Wyden amendment is not only anomalous; it is bad policy. It is the very kind of thing that, if Congress were to permit it to be written in to law and another attack should occur, the next 9/11 Commission will be asking why Congress tied the intelligence agencies' hands in this way. Congress can prevent such an eventuality by rejecting or at least mitigating the effect of the Wyden amendment.

One final criticism of the Intelligence Committee's bill: section 703(l) of that legislation requires intelligence agencies to annually report on "the number of persons located in the United States whose communications were reviewed." As it is written, this provision would require, for example, that if U.S. intelligence agents come into possession of an email message that was sent from overseas, even if our agents quickly concluded that the message is unimportant and they decide not to analyze or even read the message, they would still be required to analyze whether any of the email addresses to which the message was directed belong to a person who is located inside the United States. As the Administration's formal policy statement regarding this bill notes, "[t]his provision would likely be impossible to implement." Ken Wainstein concurred in this point in his October 31 testimony, noting that "[g]iven the fragmentary nature of foreign intelligence collection and the limited amount of information available concerning any specific intercepted communication, I am informed that it would likely be impossible for intelligence agencies to comply with this requirement."

The Judiciary Committee bill

Some of those reading this statement may wonder why this Judiciary Committee Minority Report principally addresses the Intelligence Committee bill and devotes relatively little attention to the Judiciary Committee bill. The explanation is that at the point in time when this report is being prepared—when the legislation is already under consideration on the Senate floor—it is generally expected that the Senate will only act on the Intelligence Committee bill, and that the Judiciary Committee substitute amendment will not survive a cloture vote and will thereby fall off the bill. It has been made clear that the Director of National Intelligence, the Attorney General, and other senior intelligence advisors would recommend to the President that he veto the Judiciary Committee bill should it reach his desk. Nevertheless, the Judiciary Committee bill merits a few words.

The Judiciary Committee bill includes an "exclusive means" provision that could (and probably would) undermine intelligence gathering directed at foreign terrorist organizations. The provision not only uses vague terms whose meaning is unclear, it also appears to preclude use of other intelligence-gathering tools that have already proven to be a valuable source of intelligence about al-

Qaida. As the official Statement of Administration Policy for this bill notes:

> Consistent with current law, the exclusive means provision in the SSCI's bill addresses only "electronic surveillance" and "the interception of domestic wire, oral, and electronic communications." But the exclusive means provision in the Judiciary Committee substitute goes much further and would dramatically expand the scope of activities covered by that provision. The Judiciary Committee substitute makes FISA the exclusive means for acquiring "communications information" for foreign intelligence purposes. The term communications information" is not defined and potentially covers a vast array of information—and effectively bars the acquisition of much of this information that is currently authorized under other statues such as the National Security Act of 1947, as amended. It is unprecedented to require specific statutory authorization for every activity undertaken worldwide by the Intelligence Community. In addition, the exclusivity provision in the Judiciary Committee substitute ignores FISA's complexity and its interrelationship with other federal laws and, as a result, could operate to preclude the Intelligence Community from using current tools and authorities, or preclude Congress from acting quickly to give the Intelligence Community the tools it may need in the aftermath of a terrorist attack in the United States or in response to a grave threat to the national security. In short, the Judiciary Committee's exclusive means provision would radically reshape the intelligence collection framework and is unacceptable.

To cite just one example of the damage that the Judiciary Committee's "exclusive means" provision could do, it is unclear whether intelligence about terrorist organizations could still be gathered under that provision through the use of grand-jury subpoenas. The "exclusive means" provision requires that foreign-intelligence-gathering tools have "specific statutory authorization." Grand-jury subpoenas are authorized by the Federal Rule of Evidence. Arguably, the Federal Rules themselves are authorized by statute, and thus so, too, are grand-jury subpoenas. (Though is such derivative authorization "specific?") Grand-jury subpoenas have proven a very valuable tool in counterterrorism investigations; they were the source of some of the United States's first intelligence about al-Qaida, intelligence that was gathered in the course of the 1993 Trade Center bombing trial and investigations of al-Qaida attacks during the 1990s. The fact that the Judiciary Committee bill even creates a question as to whether antiterrorism investigators could continue to employ grand-jury subpoenas to track al-Qaida strongly suggests that this legislation is poorly thought out.

Another fatal flaw in the Judiciary Committee bill is its failure to provide protection to private parties who have assisted the government in past terrorism investigations—and whose assistance the United States will need in future investigations. As the SAP on the Judiciary Committee bill notes, the failure to provide such pro-

tection undermines U.S. efforts to respond to and stop al-Qaida in two ways: first, it allows the continuation of litigation that has already resulted in leaks that have done serious damage to U.S. counterterrorism efforts. This litigation is inherently and inevitably damaging to U.S. efforts to monitor al-Qaida's communications. As one Intelligence Committee staffer aptly characterized the situation, allowing this litigation to go forward is the equivalent of allowing the legality of the enigma code-breaking system to be litigated during World War II.

In addition, the failure to provide protection to third parties who have assisted the United States will undermine the willingness of such parties to cooperate with the government in the future. And such cooperation is essential to U.S. efforts to track al-Qaida. As the SAP on the bill explains:

> In contrast to the Senate Intelligence Committee bill, the Senate Judiciary Committee substitute would not protect electronic communication service providers who are alleged to have assisted the Government with communications intelligence activities in the aftermath of September 11th from potentially debilitating lawsuits. Providing liability protection to these companies is a just result. In its Conference Report, the Senate Intelligence Committee "concluded that the providers * * * had a good faith basis for responding to the requests for assistance they received." The Committee further recognized that "the Intelligence Community cannot obtain the intelligence it needs without assistance from these companies." Companies in the future may be less willing to assist the Government if they face the threat of private lawsuits each time they are alleged to have provided assistance. The Senate Intelligence Committee concluded that: "The possible reduction in intelligence that might result from this delay is simply unacceptable for the safety of our Nation." Allowing continued litigation also risks the disclosure of highly classified information regarding intelligence sources and methods. In addition to providing an advantage to our adversaries by revealing sources and methods during the course of litigation, the potential disclosure of classified information puts both the facilities and personnel of electronic communication service providers and our country's continued ability to protect our homeland at risk. It is imperative that Congress provide liability protection to those who cooperated with this country in its hour of need.
>
> The ramifications of the Judiciary Committee's decision to afford no relief to private parties that cooperated in good faith with the U.S. Government in the immediate aftermath of the attacks of September 11 could extend well beyond the particular issues and activities that have been of primary interest and concern to the Committee. The Intelligence Community, as well as law enforcement and homeland security agencies, continue to rely on the voluntary cooperation and assistance of private parties. A decision by the Senate to abandon those who may have provided assistance after September 11 will invariably be

noted by those who may someday be called upon again to help the Nation.

The Judiciary Committee bill also includes a provision that would limit FISA overseas intelligence gathering to "communications to which at least 1 party is a specific individual target who is reasonably believed outside of the United States." One implication of this provision is that if the U.S. military were planning to enter and occupy an enemy-occupied city in Iraq, and the night before the invasion the commanding officer asked that all communications into or out of the city be monitored, FISA would bar such surveillance. The enemy forces inside the city, unless identified as including at least one "specific individual target," would have privacy rights against the United State Army, courtesy of the U.S. Congress.

The Majority Report for this bill, at subsection 6, attempts to back away from the implications of this provision. The Report states: "The Committee also wants to make clear that in an active or projected zone of military combat the acquisition of communications of any target, known or unknown, would be deemed to have a foreign intelligence purpose by virtue of geographic location if such acquisition is tailored to support such military operations."

The text of the Judiciary Committee bill, of course, contains no such "military zone" exception. Committee reports can explain legislative language but they cannot amend it. We nevertheless take comfort in this statement in the Majority Report, as it suggests that even the Committee Majority has concluded that the natural and obvious implications of this provision of the Judiciary Committee bill are indefensible.

Finally, we would note in passing that the first paragraph of the Majority Report's explanation of the purpose of this bill asserts that telecommunications companies' assistance to the United States—and, by implication, the entire program of post-September 11 warrantless surveillance of al-Qaida communications—was "contrary to law." Yet as the quotation from the FISA Court of Review at the beginning of this dissent notes, every court that has considered the question has concluded that the President *does* have inherent authority under the Constitution to gather information about foreign enemies of the United States without a warrant. The Majority Report cites no authority to the contrary, and there is no such authority. Indeed, every Administration since FISA was enacted—including the Carter Administration—has concluded that Congress cannot take away the President's power to monitor foreign enemies of the United States without a warrant, and that to the extent that FISA purports to do so, it is unconstitutional. The Constitution's framers vested the executive with primary responsibility and authority to protect the United States from foreign attack. The severe flaws in the Judiciary Committee bill, noted here and elsewhere, tend to confirm the wisdom of this approach.

Why this matters

Many of those defending various legal limits on counterterrorism investigations assume or even explicitly assert that these limits are simply procedural—that such limits only require intelligence agen-

cies to jump through a few extra hoops, and that in the end the job will still get done.

One pre-September 11 investigation in particular offers a cautionary tale as to why we should not assume that arbitrary legal barriers will not fatally compromise a critical antiterrorism investigation. The investigation in question involved Khalid al-Mihdhar. Al-Mihdhar was one of the eventual suicide hijackers of American Airlines Flight 77, which was crashed into the Pentagon, killing 58 passengers and crew and 125 people on the ground.

An account of a pre-September 11 investigation of al-Mihdhar is provided in the 9/11 Commission's *Staff Statement No. 10.* That statement notes as follows:

> During the summer of 2001 a CIA agent asked an FBI official * * * to review all of the materials from an al Qaeda meeting in Kuala Lumpur, Malaysia one more time. * * * The FBI official began her work on July 24 of 2001. That day she found the cable reporting that Khalid Al-Mihdhar had a visa to the United States. A week later she found the cable reporting that Mihdhar's visa application—what was later discovered to be his first application—listed New York as his destination. * * * The FBI official grasped the significance of this information.
>
> The FBI official and an FBI analyst working the case promptly met with an INS representative at FBI Headquarters. On August 22 INS told them that Mihdhar had entered the United States on January 15, 2000, and again on July 4, 2001. * * * The FBI agents decided that if Mihdhar was in the United States, he should be found.

At this point, the investigation of Khalid al-Mihdhar came up against the infamous legal "wall" that separated criminal and intelligence investigations at the time. The Joint Inquiry Report of the House and Senate Intelligence Committees describes what happened next:

> Even in late August 2001, when the CIA told the FBI, State, INS, and Customs that Khalid al-Mihdhar, Nawaf al-Hazmi, and two other "Bin Laden-related individuals" were in the United States, FBI Headquarters refused to accede to the New York field office recommendation that a criminal investigation be opened, which might allow greater resources to be dedicated to the search for the future hijackers. * * * FBI attorneys took the position that criminal investigators "CAN NOT" (emphasis original) be involved and that criminal information discovered in the intelligence case would be "passed over the wall" according to proper procedures. An agent in the FBI's New York field office responded by e-mail, saying: "Whatever has happened to this, someday someone will die and, wall or not, the public will not understand why we were not more effective in throwing every resource we had at certain problems."

The 9/11 Commission has reached the following conclusion about the effect that the legal wall between criminal and intelligence in-

vestigations had on the pre-September 11 investigation of Khalid al-Mihdhar:

> Many witnesses have suggested that even if Mihdhar had been found, there was nothing the agents could have done except follow him onto the planes. We believe this is incorrect. Both Hazmi and Mihdhar could have been held for immigration violations or as material witnesses in the Cole bombing case. Investigation or interrogation of these individuals, and their travel and financial activities, also may have yielded evidence of connections to other participants in the 9/11 plot. In any case, the opportunity did not arise.

The USA Patriot Act later dismantled the legal wall between intelligence and criminal investigations. But were the Congress to enact the Judiciary Committee's FISA bill, or impose other arbitrary limits on overseas intelligence gathering, it would be erecting new walls that would unnecessarily burden counterterrorism investigations and compromise U.S. efforts in the war against al-Qaida. These types of bureaucratic barriers matter. They may have fatally undermined the best chance that the United States had of uncovering or at least disrupting the 9/11 plot. We should learn from the mistakes of the past.

Conclusion

We conclude by asking: what is the Congress's goal? Do we want to allow our intelligence agencies to use the most up-to-date technology to track and prevent attacks by the most evil people in the world today, al-Qaida terrorists, or are we so concerned about some potential, theoretical situation in which an American citizen's communications might be temporarily intercepted, if they call an al-Qaida person or an al-Qaida person calls them, that we are not going to take advantage of these intelligence-collection techniques?

We can write the law to ensure the protection of every U.S. person against surveillance abuses. We need to do that. But we should not restrict our intelligence agencies from collecting the available and accessible intelligence that might warn us of another terrorist attack.

JON KYL.
ORRIN G. HATCH.
CHUCK GRASSLEY.
JEFF SESSIONS.
LINDSEY GRAHAM.
JOHN CORNYN.
TOM COBURN.
SAM BROWNBACK.

E. MINORITY VIEWS OF SENATOR HATCH

As the only Republican Senator on both the Intelligence and Judiciary Committees, I have witnessed the evolution of this bill through both committees.

The Judiciary substitute is deficient to accomplish the purpose of protecting our nation for a myriad of reasons, primarily for the fact that it contains numerous provisions which will harm national security. But to put it in one simple phrase, the Judiciary substitute lacks balance.

The Judiciary Committee received a bipartisan bill which had been approved 13–2. However, after deliberations the final Judiciary Committee substitute included 13 substantive changes, all of which were approved by a party line 10–9 vote.

Does that sound balanced? Does it sound like the Judiciary Committee exhibited a willingness to work together?

Fueled by disappointment with the process in the committee, I joined seven other Republican Senators on the Judiciary Committee to send a letter to Senate Leadership expressing our support for the FISA bill as passed out of the Intelligence Committee to serve as the basis for floor debate. I can guarantee that the other Senators took no joy in recommending a bill from another committee over the one in which they serve, but the end product produced by the Judiciary Committee gave them no choice.

Some have expressed support for the Judiciary Substitute because they think it has increased oversight.

Are people aware of the extensive amount of oversight that is included in the bipartisan Intelligence Committee FISA modernization bill? Here are some provisions:

- Foreign Intelligence Surveillance Court (FISC) review of AG/DNI certifications.
- FISC review of targeting procedures.
- FISC review of minimization procedures.
- Statutorily required AG/DNI semiannual assessment of compliance with targeting and minimization procedures.
- Statutorily required Inspector General semiannual assessment of compliance with targeting and minimization procedures.

The bill also includes:

- Annual reviews to be conducted by the head of each IC element conducting acquisitions.
- Statutorily required Attorney General semiannual report to Congress regarding implementation.

Seeing this dramatic expansion in FISC jurisdiction, it's important to realize what it was created for. The jurisdiction of the FISC is to grant orders for electronic surveillance. That's it. Many of the oversight provisions represent a dramatic departure from the original intent of FISA, which was to apply oversight and protections

to domestic surveillance. This bill is greatly expanding oversight of foreign surveillance.

I believe this expansion of FISC jurisdiction is unnecessary. Since the creation of the National Security Agency, American intelligence analysts have had the authority and responsibility to conduct surveillance and abide by our laws. These analysts all pass an extensive background check to receive security clearances. They are not politically appointed, and they continue to serve regardless of who the current President may be, or which political party is in power. They all take an oath to defend the Constitution of the United States. Their integrity is beyond dispute, and yet we continue to push proposals that treat them as if they can't be trusted. These analysts don't need more oversight, they need us to give them the tools necessary to prevent the next terrorist attack.

Despite my concerns with this issue, I am still fully supporting the Intelligence Committee FISA modernization bill over the Judiciary substitute. This is because I understand what it means to compromise. Do I wish there were additional changes? Absolutely. But I've served long enough to know that legislation, especially national security legislation, requires compromise to ensure passage.

Personally seeing the transformation of the bill between the two committees has made my opinion crystal clear. I will support the bill which passed the intelligence committee 13–2, and will adamantly oppose the partisan Judiciary Substitute if it is offered as a substitute on the Senate floor.

ORRIN G. HATCH.

ATTACHMENT

December 4, 2007.

Hon. HARRY REID,
Senate Majority Leader,
Washington, DC.

Hon. MITCH MCCONNELL,
Senate Minority Leader,
Washington, DC.

DEAR MAJORITY LEADER REID AND MINORITY LEADER MCCONNELL: As the Senate prepares to debate Foreign Intelligence Surveillance Act (FISA) modernization legislation, we want to state our collective support for the bipartisan legislation (S. 2248), drafted by Chairman Rockefeller and Vice Chairman Bond and reported by the Senate Select Committee on Intelligence (SSCI), serving as the basis for floor debate.

The Rockefeller-Bond bill represents a bipartisan attempt to craft legislation which would provide critical intelligence-gathering authority to the Intelligence Community, while providing appropriate oversight by Congress, the Foreign Intelligence Surveillance Court, and the Executive Branch. The Rockefeller-Bond bill was drafted after careful and lengthy negotiations between Democratic and Republican staff on the Intelligence Committee. The legislation includes important input from the Director of National Intelligence, the Department of Justice, and the Intelligence Community as a whole. These efforts resulted in a balanced bill which was reported by the SSCI by an overwhelming 13–2 bipartisan vote.

In stark contrast, the substitute bill reported by the Senate Judiciary Committee does not reflect the same bipartisan spirit. Following committee referral and during a Judiciary Executive Business Meeting, a substitute amendment offered by Senator Leahy was adopted after little debate by a slim 10–9 party-line vote. The Leahy substitute replaced the entire Intelligence Committee bill and completely disregarded the delicate compromises contained in the bipartisan bill.

The Leahy substitute, when narrowly approved by the Democrats on the Judiciary Committee, contained 10 separate Democratic amendments and no Republican amendments. The Intelligence Community expressed great concern before the Judiciary Committee's markup—and indeed continues to express such concern—with many of the amendments included in the Judiciary bill. These concerns prompted Attorney General Mukasey and Director of National Intelligence McConnell to send a joint letter to the Chairman and Ranking Member of the Judiciary Committee as well as the Chairman and Vice Chairman of the SSCI stating, "If the substitute is part of a bill which is presented to the President, we and the President's other senior advisers will recommend that he veto the bill." While this letter reflected the views of the Intelligence Community on the earlier version of the Leahy substitute, most of these concerns still apply to the substitute as reported, which contains provisions that could limit intelligence collection and national security investigations.

Furthermore, three additional Democratic amendments were adopted via party-line votes during the markup. Some of these

amendments could lead to very serious unintended consequences for our Intelligence Community, hampering its ability to protect American citizens from terrorists. For example, one amendment would prevent the military from monitoring all electronic communications into and out of foreign cities or compounds prior to American military invasion. This presents a risk to the safety of our troops that is simply unacceptable.

The Rockefeller-Bond legislation also contains important immunity provisions for those telecommunications carriers alleged to have assisted the U.S. Government after the September 11th terrorist attacks. During the Judiciary business meeting, an amendment to strike these immunity provisions was rejected by a 12–7 bipartisan vote. However, in a move which nullified the committee's 12–7 vote, Chairman Leahy called for a subsequent vote on favorably reporting only Title I of the Leahy substitute, thus striking titles II and III of the Rockefeller-Bond legislation. This motion passed on a party-line 10–9 vote. This vote not only removed the retroactive immunity provisions, but also removed vital procedures for implementing future statutory defenses, a severability clause, and procedures for transitioning from the Protect America Act. This leaves the final bill reported by the Judiciary Committee with an amalgamation of unworkable and ill-defined procedures for the Intelligence Community to follow, combined with poor public policy which could cripple our nation's ability to effectively gather intelligence and protect our citizens from harm.

As you know, in order for FISA legislation to successfully pass the Senate and be enacted into law, it will need bipartisan support and the backing of those trusted to protect U.S. interests in the Intelligence Community.

We therefore reiterate our support for the Rockefeller-Bond legislation as passed by the SSCI. Such support, however, should not be construed as endorsement of every facet of the bill, as we recognize that there are significant concerns with a few provisions in the bill that will need to be addressed on the Senate floor. However, we remain confident that these issues can be resolved in a timely manner so that our nation's intelligence personnel can spend their time protecting Americans from the forces of evil around the world.

In our opinion the Rockefeller-Bond legislation holds the greatest promise for bringing the Senate together and getting a FISA bill enacted swiftly. As you well know, we must act efficiently and responsibly to ensure that the dedicated men and women in the Intelligence Community have the tools and authority they need to effectively collect foreign intelligence information.

Sincerely,

LINDSEY GRAHAM.
TOM COBURN.
SAM BROWNBACK.
JON KYL.
ORRIN HATCH.
JEFF SESSIONS.
JOHN CORNYN.
CHARLES GRASSLEY.

X. Changes to Existing Law Made by the Bill, as Reported

In the opinion of the Committee, it is necessary to dispense with the requirements of paragraph 12 of rule XXVI of the Standing Rules of the Senate in order to expedite the business of the Senate.

○